

REMARKSRECEIVED
CENTRAL FAX CENTER

The Applicants request reconsideration of the rejection.

JUL 20 2007

Claims 1-8 and 18-22 are now pending, including new claims 18-22, which were submitted in the "Preliminary Amendment" dated November 24, 2006, but not entered. The Applicants note that claim 18 has been amended to correct an editing error in the claim as filed November 24, 2006.

Claims 1-8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the Applicants' admitted prior art in view of Jaffe et al., U.S. Patent No. 6,510,518 (Jaffe). The Applicants respectfully traverse, and address the Examiner's comments found on pages 3-7 of the Office Action, as follows.

As previously argued (see the Preliminary Amendment filed November 8, 2006), independent claim 1 recites that the input data D1 and the processed transformed data H2 are each disturbed by constant-hamming-weight disturbance data, whereas the prior art disturbance data is not required to have a constant hamming weight. Therefore, even in any motivated combination with Jaffe, the prior art would not lead the person of ordinary skill to the invention claimed in claim 1.

The Applicants requested the Examiner to consider the result of the person of ordinary skill attempting to modify the admitted prior art according to Jaffe. In making the request, the Applicants provided several proposals as to the result of attempting to modify the admitted prior art according to Jaffe. Specifically, the Applicants suggested that because Jaffe maps input data (D1; all data indicators are referenced to the present specification's terminology for convenience) to obtain data H1, and the admitted prior art disturbs input data D1 with disturbance data Y1 to obtain data H1, if one of ordinary skill were to apply the mapping of Jaffe to the

teachings of the admitted prior art, one would seem to map the input data D1, for example, before disturbing D1 with disturbance data Y1, or perhaps one would disturb D1 with the disturbance data Y1 and then map the resulting data to obtain H1 with a constant hamming weight.

However, as noted by the Applicants, the former example (i.e., mapping D1 prior to disturbing it) would already achieve the result sought by Jaffe, namely, H1 with a constant hamming weight. Thus, there would be required a teaching of the subsequent disturbance with disturbance data Y1 having a constant hamming weight, to achieve the claimed invention. However, Jaffe does not teach to map twice and thus this example seems to be insufficient to render obvious the claimed invention.

Applying Jaffe according to the second example is likewise different from the claimed invention. According to the claimed invention, the disturbance data itself has a constant hamming weight. If the person of ordinary skill were to map the disturbed data according to the suggestion of Jaffe (parenthetically, the Applicants do not admit that such a mapping is suggested), the disturbance data itself would not have constant hamming weight as required by the claims. Thus, even in this example, the claimed invention is not met by any combination of the admitted prior art and Jaffe.

Against these arguments, the Examiner alleged that the Applicants' assertion "is merely a broad supposition or allegation by Applicant of what would result from the combination, which would result from bodily combining the steps of Jaffe with the steps of the admitted prior art, rather than the modifications of the admitted prior art that would be suggested to one of ordinary skill by the teachings of Jaffe. However,

the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the [text missing from Office Action]. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art" (citing *In re Keller*, 642 F.2d 413, 208, USPQ 871 (CCPA 1981)). The Applicants note, however, that their proposals are an attempt to focus the issue of just what the allegedly combinable teachings of the references would have suggested to ordinary skill in the art. The rejection itself simply alleges to modify the admitted prior art to include constant-hamming-weight data, without so much as even "bodily incorporating" any teachings of Jaffe into the admitted prior art. Indeed, the rejection does not explain, except to use the claim as a roadmap, what the result of modifying the admitted prior art according to Jaffe would be. The Applicants' proposals consider how the person of ordinary skill would modify the admitted prior art according to Jaffe, and what the result might be. Thus, the Applicants request the Examiner to indicate the result of combining Jaffe with the admitted prior art, using those teachings, rather than the claim, as a roadmap.

Further, the Examiner also alleged that the Applicants' proposals do not provide citations to the prior art in support of the proposals. Of course, there are no citations to the prior art in support of the proposals; the prior art does not suggest the combination, despite the assertion in the rejection. The proposals were the Applicants' attempt to consider the rejection in the most favorable light to the Examiner's position. The Applicants respectfully submit that the mapping taught by Jaffe, if applied in an attempt to modify the admitted prior art, might result in one or

the other proposals outlined in the Applicants arguments. In this regard, the Applicants refer the Examiner to the remarks accompanying the Reply filed October 16, 2006, incorporated into the remarks filed November 8, 2006 (see page 8 and page 9 for the Applicants' specific requests).

Regarding the paragraph bridging pages 4 and 5 of the Office Action, which essentially constitutes a restatement of the Examiner's prior position, the Applicants, in turn, reassert their prior arguments that Jaffe does not contain teachings so broad so as to suggest to one of ordinary skill to use a constant hamming weight representation for all data within a system such as the one admitted as prior art, and thus a person of ordinary skill would not be motivated to modify the admitted prior art according to Jaffe, and that such a combination would not reach the claimed invention, absent the hindsight reasoning set forth in the bridging paragraph.

Claims 2-8 are distinguished as before. The Applicants incorporate by reference all arguments previously presented.

Concerning new claims 18-24, the Applicants again note that none of the documents of record, whether taken individually or in any motivated combination with each other, or with the admitted prior art, is believed to disclose or fairly suggest the evaluation of the hamming weight of the processed second disturbance data or the concatenation of the m-bit random numbers randomly into an n-bit random number which is used as the first disturbance data. In particular, no document of record recognizes the value of first disturbance data having a constant hamming weight, or the reduction in time required for evaluating the hamming weight of the first disturbance data by ensuring that the n-bit random number (from which the m-bit first disturbance data is produced) has a constant hamming weight.

By way of example, the Applicants specifically refer to paragraph [0095] of the published application U.S. 2002/0154767, corresponding to page 26, lines 2-20 of the present specification, for support. In the embodiment disclosed therein, a hamming-weight evaluation method 505 is used for evaluating a hamming weight of the X₁₀ processed disturbance data 504. No reference of record discloses this evaluation process because the references of record do not consider the hamming weight of the disturbance data. Similarly, the references do not address the concatenation of the m-bit random numbers randomly into an n-bit random number which plays the role of the disturbance data, as disclosed, for example, in paragraph [0099] of the '767 publication (corresponding to page 28, line 25 – page 30, line 9). The present invention is effective in reducing the evaluation time in accordance with the concatenation, etc. performed by the claimed processor, because it takes a long time to judge whether the hamming weight of the generated n-bit random number R is equal to the target hamming weight H (see item 704, Fig. 7), particularly as the generated random number R becomes larger. The present invention does not require the judging process, because the m-bit random numbers are generated in advance with uniform constant hamming weights.

Thus, the prior art does not disclose or fairly suggest the information processing apparatus claimed in claim 18, including a processor arranged to carry out processing operations, a storage arranged to store programs and data, and a data bus which interconnects the processor and the storage, wherein wherein the processor is further arranged to generate m-bit random numbers having a predetermined hamming weight, concatenate the predetermined number of the m-bit random numbers randomly into first disturbance data of n bits equal to a multiple of

process the first disturbance data with a first operation, generate second disturbance data, and evaluate whether the second disturbance data has a target hamming weight; and wherein the processor is further arranged to transform input data into first transformed data with the first disturbance data, process the first transformed data with the first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data.

Further, as set forth in new dependent claim 19, the prior art does not disclose an information processing apparatus as claimed in claim 18 and argued above; wherein the appearance probabilities of the logic value 0 or 1 at each bit position of the first disturbance data and the second disturbance data are set at 50%. The prior art also does not suggest the limitation of dependent claim 20, which requires the m-bit random numbers to be collected in a table.

In addition, the prior art does not suggest the information processing apparatus set forth in dependent claim 21, wherein the processor of claim 18 argued above is arranged to transform the input data into the first transformed data by means of either one of an XOR operation, an addition operation, or the transform operation with the first disturbance data. The prior art also does not suggest the limitation of dependent claim 22, which requires the first operation to be either one of a rotate operation, a shift operation, or a bit permutation operation.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing

07-20-'07 15:01 FROM-Mattingly, Stanger

703-684-1157

T-261 P017/020 E-396

U.S. Application No. 09/940,982

of this paper, including extension of time fees, or credit any overpayment of fees, to
the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account
No. 50-1417 (referencing attorney docket no. NIT-295).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120